International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209706 Volume 8, Issue 4, July – August (2021)

RESEARCH ARTICLE

Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E

Valanto Alappatt
Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India.
alappatvalanto@gmail.com

Joe Prathap P M
Department of Information and Technology, RMD Engineering College, Chennai, India.
drjoeprathap@gmail.com

Received: 03 July 2021 / Revised: 24 July 2021 / Accepted: 29 July 2021 / Published: 28 August 2021

Abstract – Multipath Routing (MR) technique is much common in Mobile Ad-hoc Networks (MANET) as they overcome single-path routing's particular limitations. However, by reason of the deficiency of trusted centralized authority and also inadequate resources, attaining energy-effective secure MR is a significant challenge in MANET. Aimed at overcoming these challenges, this work proposes a trust-centred energy-efficient MR scheme for MANET. In this research, primarily, the direct and indirect trust of nodes and paths are examined and centred on these trust values, the secure multipath is selected and also the victim nodes are identified and isolated. Next, the data packets (DPs) are encrypted using the Secret key-centred Hybrid Honey Encryption (SH2E) algorithm to secure the DPs against data transmission (DT) attacks. Next, the Levy Flight centred Shuffled Shepherd Optimization (LF-SSO) Algorithm is applied to discover an optimal path as of the multipath selected. This algorithm improves the network's lifetime by discovering a path based on path trust, residual node energy, and also the path's distance. And then, the encrypted DPs are forwarded as of the source node (SN) onto the destination node (DN) over the discovered optimal path, and finally, transmitted to the base station (BS). This work not only considers the energy-efficient secure routing but also considers the route maintenance. The experiential outcomes are given to exhibit the proposed system's efficacy.

Index Terms – Encryption, Energy, Multipath Routing, Mobile Ad Hoc Networks, Optimization, Routing.

1. INTRODUCTION

Recently, MANET has progressed as one amidst the fastest-developing fields of research and more common technology in the wireless network (WN) as a consequence of the incremented wireless devices' adoption [1]. A MANET is defined as an assembly of wireless devices traveling in apparently arbitrary directions and communicating with each other with no assistance from a developed infrastructure [2]. Communicating nodes prevalent in a MANET generally pursue other intermediate nodes' aid aimed at developing communication channels [3]. MANET routing protocols function as a fundamental element in ubiquitous devices' potential future [4]. Routing protocols are generally categorized as on-demand, table-driven (proactive), and also hybrid. As for frequent network change, an on-demand approach is preferred for many MR in MANET [5].

Recently, on-demand MR approaches have become important research in MANET. The MR approaches provide numerous routes betwixt a source-destination pair. Multipath techniques comprise numerous advantages, like higher bandwidth utilization, higher network life, lesser end-to-end delay, higher throughput, et cetera [6]. It decreases network congestion and protection against route failures [7, 8]. The foremost challenging task to offer an on-demand MR scheme aimed at mobile ad-hoc networks is to attain a secure protocol by maintaining the trust and also energy efficacy simultaneously.

NOMENCLATURE			
MR	Multipath Routing	AOMDV	Ad-hoc On-Demand multipath Distance Vector
MANET	Mobile Ad-hoc Networks	AODV	Ad-hoc On-Demand Distance Vector
DPs	Data Packets	EA-MPDSR	Energy-Aware Multi-Path Dynamic Source Routing
SH2E	Secret key-centred Hybrid Honey Encryption	EMRP	Energy-aware MR Protocol
LF-SSO	Levy Flight centred	RSA	Rivest–Shamir–Adleman

	Shuffled Shepherd Optimization		
DN	Destination Node	RREQ	Route Request
BS	Base Station	RREP	Routing Reply
WN	Wireless Network	DTD	Distribution Transforming Decoder

Table 1 Nomenclature

Aimed at ensuring the work, diverse secured routing protocols in MANETs, like cryptographic approaches [9] and game-theoretic approaches [10, 11] are established in the former years. The cryptographic approach is trust-centred mechanisms not generic to be utilized in all MANET types. [12]. Game theoretic-centred security, defence mechanisms, and decision-making protocols can be utilized in resource-constrained networks.

Nevertheless, these techniques' performance worsens whilst implemented in an unfavorable MANET's environment and whilst the attackers are energy-efficient and adaptive in nature. Aimed at providing an energy-efficient approach in MR in MANET, an energy management protocol is utilized [13]. An energy-aware MR protocol has to maintain a trade-off betwixt energy consumptions (ECs) and other metrics, such as link reliability, network capacity, throughput, end-to-end delay, etc.

Recently, the existent researches, like MMRE-centred on Ad-hoc On-Demand multipath Distance Vector (AOMDV) [14], Ad-hoc On-Demand Distance Vector (AODV) [15], AOMDV [16], a cross-layer optimized Energy-aware MR Protocol (EMRP) [17], and Energy-Aware Multi-Path Dynamic Source Routing (EA-MPDSR) protocol [18] was established to offer an energy-efficient effective on-demand technique. [19].

Additionally, in the data flow attacks' presence, like intercepting, jamming, and also hijacking, the existent work doesn't perform effectively. Generally, during the data-transfer as of an SN onto a DN, an apt path selection is of supreme significance. An excellent path is essential to upgrade EC, guarantee the DPs' secured delivery, and balance the load of a MANET's intermediate nodes. Hence, this work proffers a trust-centred energy-efficient MR scheme aimed at trying and attaining all aforesaid objectives.

The motivation of this research is to obtain energy-efficient secure MR in MANET is a big issue due to a lack of trusted centralised authority and also insufficient resources. The objective of this research is to offer a trust-centered energy-efficient MR strategy for MANET to address the issues. The detailed nomenclature used in this paper is shown in table 1. This paper's remaining part has been systematized as: Section 2 exemplifies the related work. Section 3 comprehensively elucidates the proposed energy-effective secured MR in a comprehensive manner with apt diagrammatic depiction. Section 4 exhibits the proposed methodology's outcomes and also a discussion. Section 5 completes the research with its future work.

2. RELATED WORK

Rajashanthi *et al.* [20] established an innovative Quality of Service (QoS) dependant secured MR system aimed at dependable data communication and also encryption methodologies. Likewise, the MR procedure AODV-BR technique with Optimal Fuzzy Logic was pondered. The Grey Wolf Optimization approach's Adaptive formation of envisioned the optimal path. Hence, an optimal path was chosen as of the recognized routes aimed at sheltering the data key management methodologies. The simulation outcome validated that the recommended work's energy efficacy and network lifetime were developed better than that of existing work. But for a secured MANET, a trade-off betwixt the services should be offered that means if one service guarantees with not noticing other services, the security system would fail.

Kasthuribai *et al.* [21] presented a secured and QoS centred energy-aware MR in MANET. Aimed at selecting multipath route, a particle swarm optimization-gravitational search technique was employed. Centred on the algorithm, in the network, energy-efficient multipath routes were chosen. As of the developed routes, an optimal path was chosen in the network centred on the cuckoo search technique that performed centred on cuckoos' behavior. Simulation outcomes exhibited that the work's energy efficacy and network security was enhanced analogized to that of the existent work. Due to diverse factors, network topologies repeatedly vary that consecutively causes network failures.

Veeraiah *et al.* [22] exemplified an efficient MR technique in MANET centred on an optimization technique. In the MANET, the energy and also the security issues were efficiently addressed with the cluster-head's (CH's) selection and also intrusion detection stratagems, like, fuzzy clustering and also fuzzy Naïve-Bayes (NB). Bird swarm-whale optimization algorithm (BSWOA) that was birds swarm optimization's (BSA's) integration in whale optimization algorithm (WOA) was utilized to attain optimal routing protocol. The BSWOA attained the throughput, maximum energy, a minimal delay, and detection rate in the attack's presence. This restriction signifies the time required aimed at every technique to discover malevolent nodes and also secure the networks against every malevolent node.

Muthurajkumar *et al.* [23] developed a secured routing technique termed Cluster-centred Energy-Efficient Secure

Routing Algorithm (CEESRA) that was energy-effective and utilized cluster-centred routing where the trust scores on nodes were utilized aimed at effectively detecting the intruders. The routing algorithm decremented the Service attacks' Denial much effectively with intelligent agents aimed at efficient decision making in routing. As of the experimentations executed with this trust-centred secured routing technique, it had been perceived that the routing technique not just boosted the security however also decremented the routing delay and EC. Clustering can resolve a few security challenges however cluster's creation and also its maintenance were extremely challengeable owing to MANET's dynamic topology.

Taha et al. [24] highlighted the EC in MANET via the fitness function (FF) technique aimed at optimizing the EC in AOMDV routing technique. The AOMDV protocol with the FF is termed FF-AOMDV. The FF was employed aimed at discovering the optimal path as of the SN onto the DN for decrementing the EC in MR. FF-AOMDV protocol's performance had been examined with network simulator version 2 in which the performance was analogized with AOMDV and ad hoc on-demand MR with Life Maximization (AOMR-LM) techniques. Moreover, it incremented traffic overhead by sending duplicated packets. This incremented the congestion, packet loss, and EC.

K.valarmathi et al. [25] pondered the EC issue prevalent in MANET, and also it was overcome via the energy constraints' optimization. The mobile nodes prevalent in MANET had been grouped via the K-medoid clustering technique primarily that could decrement the data routing's cost in massive and also dense networks. As for every cluster, the restricted EC-centred MR was accomplished employing the opposition genetic-centred fish swarm optimization (FSO) technique. Simulation outcomes discovered that the work's energy efficacy and its network lifetime were enhanced than the existent work. However, the technique could just evade the network as an attack. But, the technique might detect an attack, in case of misbehavior, whilst they were incapable to detect the malevolent nodes or else eradicate them as of the whole network.

Sarkar et al. [26] exemplified a secured and energy-effective stochastic MR technique centred on a Markov chain aimed at MANET. The routing protocol computed numerous paths betwixt source-destination pairs and elected an energy-effective path stochastically as of those paths aimed at forwarding the DPs. Moreover, the technique as well secured the data flow prevalent in the network as the DPs were transmitted via arbitrary paths as of the SN onto the DN. The performance examination and also the numerical outcomes validated that the technique attained vital performance gains regarding the routing protocols' EC, throughput, delay, and also security. However, in the routing information defeating technique, the security approach's control packets transmission processing time incremented.

3. TRUST-BASED ENERGY EFFICIENT SECURE MR IN MOBILE AD HOC NETWORK

An assembly of mobile nodes termed MANET, acts as both routers and also hosts in an ad-hoc WN and that self-organize dynamically in a WN with not utilizing any pre-built infrastructure. By reason of the MR behaviour, the MANET is adapted in numerous applications, like military, industry, and emergency recovery. EC and also secured routing are pondered as the most challenging operation in MANET owing to the deficiency of trusted centralized authority and also limited resources. Aimed at offering energy-effective secured MR betwixt ad-hoc network nodes, this work proffers a trust-centred energy-efficient MR technique aimed at MANET. The scheme proposed comprises '4' focus areas, like trust calculation, DPs' encryption, optimal routing path discovery, and then route maintenance. Here, every node can identify the victim nodes and choose the optimized secured paths utilizing trust values, node's energy level, and also path distance. Moreover, security routing is boosted by adding in cryptographic techniques. Figure-1 exhibits the proposed work's flow diagram. MR comprises detecting multiple paths betwixt a SN and DN. These numerous paths can be utilized aimed at compensating for the MANET's dynamic and unpredictable nature. In MANET, whilst the DPs are transferred via the path comprising attack nodes, the DPs can't reach the destination. Ponder a node pair N_i and N_j communicate with one another. Whilst the node 'N_i' fails to forward the DPs that is received from N_j, it said to have shown malicious behaviour against N_j. The routing procedures aren't capable to discover and segregate victim nodes and are vulnerable to attack launched by them. So, each node's trust values are examined; and centred on these trust values, the victim nodes are eliminated aimed at preventing the MANET as of attacks, error, and also loss.

3.1. Trust Evaluation Model

It computes the node's trust value centred on the nodes' communication behavior. Each node's trust value is assigned in the range betwixt 0 and 1. Each node's trust value is assigned initially as 0.1. If the node comprises a greater number of the effective continuous packet transfer, the node's trust value can increment faster, or else, a node's trust value will decrement faster. Here, each node's trust value is examined by pondering '2' trust value types. This trust evaluation is termed as hybrid trust evaluation. The hybrid trust is signified as in equation (1),

$$H_T = \sum (D_T + I_T) \qquad (1)$$

Here, H_T implies the hybrid trust evaluation; D_T signifies the direct trust; I_T symbolizes the indirect trust.

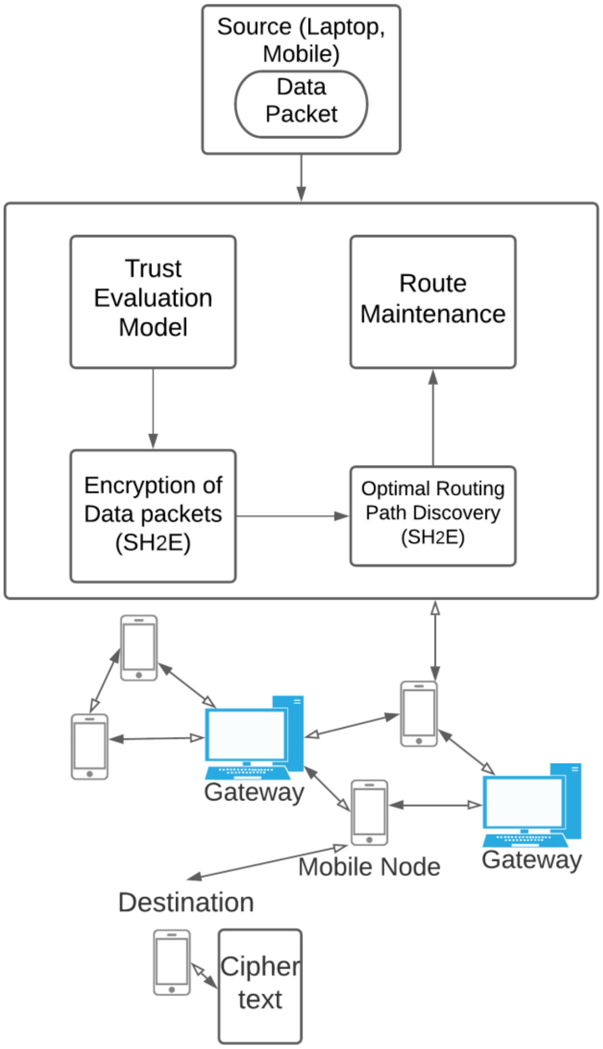


Figure 1 Proposed Flow Diagram

3.1.1. Direct Trust

It is first-hand information of direct communication among nodes and it is simple to be attained. There exist '2' direct trust types available that are node trust and path trust, which are elucidated as:

3.1.2. Node Trust

The mobile agent calculates the node trust centred on its communication range. Herein, the node trust is monitored and examined to identify if the node is forwarding or else dropping the packets. A node N_i's trust in other node N_j is a measurement to ensure that the DPs transferred by the N_i node actually are transmitted by the N_j node. The node N_i's node trust in node N_j at time step t is signified as $NT^t_{(i,j)}$ that enumerated as in equation (2),

$$NT^t_{(i,j)} = (\hat{w}_1 * R_{cf}{}^t) + (\hat{w}_2 * R_{df}{}^t) \qquad (2)$$

Herein, $R_{cf}{}^t$ and $R_{df}{}^t$ signifies the control packet forwarding ratio and DP's forwarding ratio, correspondingly at time step t; $\hat{w}_1$ and $\hat{w}_2$ implies the assigned weight values of $R_{cf}{}^t$ and $R_{df}{}^t$, correspondingly.

3.1.3. Path Trust

Path trust value's calculation is utilized to discover the path's reliability where the DPs are forwarded. This value is defined as the weighted average of the nodes' trust values in the path. The path trust is enumerated as in equation (3),

$$PT_{(i,j)} = \prod NT^t_{(i,j)} \mid N_i, N_j \in p \text{ and } N_i \to N_j \quad (3)$$

Here, $N_i \to N_j$ signifies that N_j is N_i's next hop. Lastly, the direct trust is articulated as in equation (4),

$$D_{T(i,j)} = \sum (NT_{(i,j)} + PT_{(i,j)}) \qquad (4)$$

3.1.4. Indirect Trust

It is the second-hand information regarding nodes, like a suggest trust as of a 3rd party. Aimed at boosting the trust value's accuracy, it is necessary to discover the node N_k's indirect trust as of the common adjacent nodes betwixt node N_i and N_j. The neighboring node N_k's indirect trust value to node N_j is enumerated as in equation (5),

$$I^{(k)}_{T(i,j)} = D_{T(i,k)} * D_{T(k,j)} \qquad (5)$$

Here, $I^{(k)}_{T(i,j)}$ implies the node N_i's and N_j's indirect trust value regarding N_k; $D_{T(i,k)}$ signifies the node N_i's direct trust in node N_k; $D_{T(k,j)}$ implies the node N_j's direct trust in node N_k.

The direct and indirect trust values comprise all the nodes' trust information presented betwixt SN and DN. Every node's status is identified centred on this trusted value that is exhibited in Table 2. By calculating trust values, just the nodes with efficient trust nodes are allowed aimed at communicating in the network and the victim nodes are isolated such that the MANET is capable to resist against routing attacks thrown by victim nodes. Then, the DP is encrypted at the SN for withstanding the DT attacks.

Trust Value	Node Status
$D_T < 0.5, I_T < 0.5$	Malicious Node
$D_T = 0.5, I_T = 0.5$	Suspect Node
$0.5 \le D_T \le 0.75, 0.5 \le I_T \le 0.75$	Less Trustworthy Node
$D_T > 0.75, I_T > 0.75$	Trustworthy Node

Table 2 Node Status Based On Trust Values

3.2. Encryption of Data Packets

Before transmitting the DPs as of SN to DN, the DPs are encrypted for boosting the DPs' security level against DT attacks. Converting the DPs into ciphered data is performed mainly to block unauthorized access. The system proposed utilizes the SH^{2}E algorithm. The Honey Encryption (HE) procedure is implemented aimed at executing the multi-level security in MANETS.

The HE technique is one amidst the deceive technique to attackers who utilize brute force attack. It will deter hackers by serving up fake data for the key code's every incorrect guess. The HE creates just '1' key i.e. HE key utilizing Rivest–Shamir–Adleman (RSA) technique. Aimed at boosting its security level '1' more key (i.e.) secret key is created utilizing the HE key.

For generating HE key utilizing RSA, primarily, '2' prime integers are arbitrarily elected. Ponder the '2' prime numbers as a and b, then calculate their product Q as in equation (6)

$$Q = a \times b \tag{6}$$

Next, choose '1' integer k that must be greater than '1' and less than (a-1) and (b-1). Then, the definite pair of integers Q and k forms the HE key, which is denoted as k'. Then, the HE secret key k'_S is enumerated as of the integers a, b and k' as in equation (7),

$$k'_S = k'^{-1}(a-1)(b-1) \tag{7}$$

After the key generation, HE process is executed. Let consider as the input DP as P_d. In the encryption procedure, the Distribution Transforming Encoder (DTE) is employed to the DP P_d to produce seed δ using uniform random assignment as in equation (8).

$$\delta \rightarrow \alpha DTE(P_d) \tag{8}$$

Herein, α implied the uniform random assignment. After obtaining the seed centred on HE key and random string, the seed gets encoded under a conventional encryption technique utilizing the HE key and secret key to produce the corresponding ciphertext to the DP P_d as in equation (9).

$$\hat{\delta} = H(\rho, k') \tag{9}$$

Herein, $\hat{\delta}$ signifies the encrypted seed; ρ implies the random string; H symbolizes the cryptographic hash function. Lastly, the cipher-text is attained utilizing seed and encrypted seed as in equation (10),

$$C(P_d) = (\hat{\delta} \oplus \delta) + k'_S \tag{10}$$

Herein, $C(P_d)$ signify the DP P_d's ciphertext. During encryption, the random string, encrypted seed, HE key, and secret key are sent to the receiver (authorized users) side. Utilizing these random string, encrypted seed, HE key, and secret key only, the original DP would be recovered such that just the unauthorized users can't access this ciphertext. In MR, the SN transmits this ciphertext onto the next node prevalent in the data path; it expects the next node to forward that DP. But before transmitting the ciphertext securely, it is necessary to discover a secured routing path betwixt SN and DN.

3.3. Multipath Routing Process

In MR, a SN waits for intermediate multiple paths to forward the ciphertext to the destination. In a routing discovery procedure, a SN broadcasts a route request (RREQ) message to discover the DN. whilst an intermediate node receives the RREQ message, it will record the hop count from the source to itself and forward the RREQ message to the DN. After the DN has received the RREQ message, it will begin the routing reply process and will send a routing reply (RREP) message back to the SN, and then the MR process is started.

For efficient data communication, multiple routing paths are discovered. The routing paths are generated centred on the path's trust values in this way the multi-path is built as of the SN to the DN. As the number of transaction happens in the chosen paths, there exists a possibility aimed at link quality loss. So, it is necessary to select one optimal path from the selected routing paths and the optimal path should be greatly trusted, energy-effective, and shortest as of the SN to the DN.

Thus, to acquire optimal multipath, the work proposed utilizes the LF-SSO technique centred on the factors, like the path's trust value, route energy, and also route distance.

3.4. Optimal Routing Path Discovery

An optimal routing path discovery is used to discover a better link quality path to transfer data from the SN to the DN. In this work, the optimal paths are obtained from the selected paths using the LF-SSO algorithm. The LF-SSO algorithm is a novel population-centred meta-heuristic that imitates the shepherds' herding behavior. Shepherd places horses or other animals in a group using the instinct of these animals to discover the best way to pasture. In the step size calculation process of the SSO algorithm, the horses and sheep are selected randomly. This random selection results in poor optimization. To avoid this issue, the proposed work uses a levy flight selection instead of a random selection. So, this algorithm is named an LF-SSO algorithm.

At first, a set of candidate solution is generated that contains a number of elements (i.e.) sheep. The generated candidate solution set is articulated as in equation (11),

$$\psi_j = \{\psi_1, \psi_2, \psi_3, ..., \psi_m\} \qquad (11)$$

Herein, ψ_j signifies the candidate solution set; m implies the number of sheep ($m = h \times s$); h signifies the number of group and s implies the number of sheep in every group. Then, j^{th} sheep initial position in f-dimension is articulated as in equation (12),

$$\psi_j{}^{o} = \psi_{\min} + \hat{r} \circ (\psi_{\max} - \psi_{\min}) \qquad (12)$$

Herein, $\psi_j{}^{o}$ represents j^{th} sheep's initial solution, $\psi_{\min}$ and $\psi_{\max}$ are the bound of design variables, $\circ$ implies the element-by-element multiplication and $\hat{r}$ is the random vector ($\hat{r} \in [0,1]$). Next, each solution's fitness is enumerated; herein, every candidate's solution is pondered as selected paths. Hence, each solution's fitness is pondered as maximal path trust and minimal EC and minimal path distance that is articulated in eqn. (13),

$$F_{opt} = \begin{cases} \max\left(\sum_{n=1}^{d} PT(N_n, N_{n+1})\right); & \textit{path trust} \\ \max\left(\frac{1}{N_n}\sum E_{res_n}\right); & \textit{residual energy of each node} \\ \min\left(\sum_{n=1}^{d} dist(N_n, N_{n+1})\right); & \textit{path distance betwee n source and destination} \end{cases} \qquad (13)$$

Herein, $PT(N_s, N_{s+1})$ and $dist(N_n, N_{n+1})$ signify the path's trust and path's distance betwixt node N_n and N_{n+1}, correspondingly; $n = 1$ implies SN; d signifies the DN; E_{res_n} implies the node's residual energy.

Centred on the fitness values, the solutions are sorted in ascending order. Spread the sheep to the group aimed at making the groups. In every group, the sheep are chosen in order. The sheep selected are termed shepherd and also the sheep comprising efficient fitness prevalent in a herd are termed horses. Every shepherd step-size (S_{s_j}) is computed by choosing one amidst the horse and sheep as in equation (14) and (15),

$$S_{s_j} = \omega * L^y \circ (\psi_d - \psi_j) + \varpi * L^y \circ (\psi_k - \psi_j) \qquad (14)$$

$$L^y = t(-y), \qquad 1 < y < 3 \qquad (15)$$

Herein, ψ_d and ψ_k signify the horse and sheep chosen. L^y implies the levy flight distribution; ω and ϖ imply the factors utilized to manage exploration and exploitation, correspondingly. These factors are enumerated in (16) and (17),

$$\omega = \omega_0 + \frac{\omega_{MAX} - \omega_0}{I_{MAX}} \times I \qquad (16)$$

$$\varpi = \varpi_0 + \frac{\varpi_0}{I_{MAX}} \times I \qquad (17)$$

Herein, I implies the iteration; I_{MAX} signifies the maximal iteration. This algorithm executes good exploration in early iterations and better exploitation in the final iterations aimed at attaining efficient optimization. Next, ψ_j's new position is enumerated as in equation (18),

$$\psi''_j = \psi^0_j + S_{s_j} \qquad (18)$$

If the fitness value of ψ''_j isn't worse analogized to ψ^0_j's fitness value, ψ_j's position is updated. Likewise, every path is examined and analogized with its respective old path regarding their fitness value. This process will be repeated until the optimal path is obtained. The following algorithm 1 exhibits the LF-SSO algorithm's pseudo-code aimed at optimal path selection.

```
Input: Selected Routing Paths
Output: Optimal Routing path
Begin
Initialize the candidate solution $\Psi_j$ randomly
```

```
Determine the initial position using,
$\Psi_j^0 = \Psi_{\min} + \hat{r} \circ \left(\Psi_{\max} - \Psi_{\min}\right)$
Evaluate fitness for each solution using,
$F_{opt} = \left[\left\{\begin{array}{ll} \max\left(\sum_{n=1}^{d} PT\left(N_n, N_{n+1}\right)\right); & path\ trust \\ \max\left(\frac{1}{N}\sum E_{res_n}\right); & residual\ energy\ of\ each\ node \\ \min\left(\sum_{n=1}^{d} dist\left(N_n, N_{n+1}\right)\right); & path\ disance\ between\ source\ and\ destination \end{array}\right\}\right]$
While I=0 to $I_{MAX}$ do
Sort the solutions in ascending order based on $F_{opt}$ and form group
Determine step size for each shepherd using,
    $S_{S_j} = \omega * L^y \circ \left(\Psi_d - \Psi_j\right) + \overline{\omega} * L^y \circ \left(\Psi_k - \Psi_j\right)$
Generate new elements using, $\Psi_j^n = \Psi_j^0 + S_{S_j}$
    If $\left(F_{opt}\left(\Psi_j^n\right) \geq F_{opt}\left(\Psi_j^0\right)\right)$
        sheep position = $\Psi_j^n$
    else
        sheep position= $\Psi_j^0$
    end if
end while
Return Optimal routing path
End
```

Algorithm 1 SSO Algorithm’s Pseudo-Code

Pursuing this way, the optimal path is chosen by employing this LF-SSO technique betwixt SN and DN. The optimal path signifies the path that comprises the high true value, high energy level, and also the less distance. Figure 3 exhibits the routing path’s optimal selection. Over this optimal routing path, the ciphertext is transmitted as of the SN onto the DN, and next, it is communicated securely to the BS that is explicated as in equation (19),

$$MANET \xrightarrow{Ciphertext(C(P_d))} Base\ station \tag{19}$$

After attaining the data as of the BS, the original DPs are acquired utilizing a random string, encrypted seed, HE key, and secret key that is exemplified in the section below.

3.5. Decryption of Ciphertext

The Distribution Transforming Decoder (DTD) is employed to the ciphertext in the decryption procedure proceeded by the conventional encryption technique. Next, initially, the receiver attempts to decode the encrypted seed $\hat{\delta}$ as in equation (20),

$$\delta = (C(P_d) \oplus \hat{\delta}) - k'_S \tag{20}$$

With this seed value’s assistance, the original DP is acquired utilizing the eqn. (21),

$$P_d = DTD(\delta) \tag{21}$$

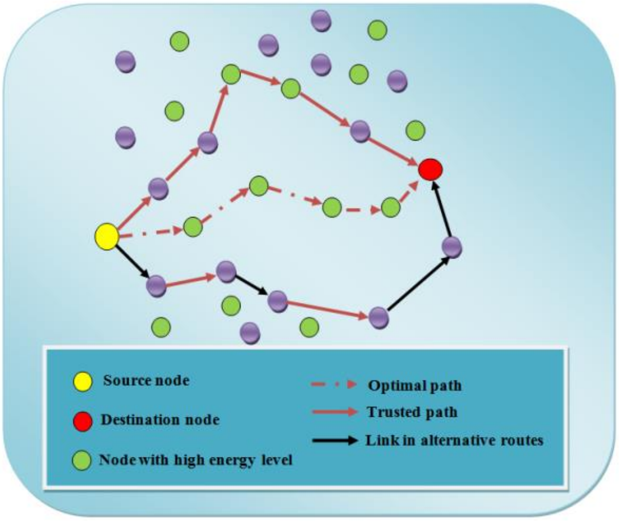


Figure 3 Optimal Routing Path Selection Process

Thus, the original DP is recovered as of the ciphered data. Only whilst the right key is implemented, the plaintext will correctly decode. When attackers try to decrypt a ciphertext with an incorrect key, HE algorithm presents a plausible-looking yet incorrect plaintext, so that a computationally unbounded adversary is still unable to distinguish whether the recovered message is valid or not.

3.6. Route Maintenance

In the route maintenance procedure, the node’s response time, energy level, and communication quality are computed over changing time intervals aimed at predicting its reliability. Whilst an intermediate node transfers a DP onto the next node, the former node is in charge to discover if its link to the upcoming hop is broken. Every node’s reliability is verified centred on its response time, energy level, and communication quality. Aimed at verification, response time, threshold energy, and threshold communication’s quality are assigned manually. If any node's energy, communication quality, and response time are below the threshold value, then the former node communicates a routing error (RERR) message onto the SN as in equation (22).

$$if \sum(E_{res},T_{res},C_q)_{Node} < \sum(E_{res},T_{res},C_q)_{Thershold},$$

$$Former\ node \xrightarrow{RERR} Source\ node \qquad (22)$$

Where, $\sum(E_{res},T_{res},C_q)_{Node}$ represents the node's current residual energy, response time and communication quality, $\sum(E_{res},T_{res},C_q)_{Thershold}$ represents the assigned threshold energy, response time and communication quality. If a SN receives a RERR, it initializes a new RREQ to the other available nodes. The route maintenance procedure boosts the performance of MANET's routing procedure.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Here, the performance of the techniques proposed utilized aimed at energy-efficient secure MR betwixt the SN and DN is examined by executing diverse experimentations on Network Simulation Tool-Version 2 (NS2). The protocols proposed, like LF-SSO and SH2E, are analogized with a few traditional existent protocols centred on a few quality metrics.

4.1. Performance Analysis of LF-SSO

In the work proposed, multipath routes are chosen centred on the path's trust values as of the network. Aimed at attaining energy-efficient secure MR, the work proposed utilizes the LF-SSO protocol, so an optimal path is chosen as of the multipath routes selected. Aimed at verifying this LF-SSO protocol's effectiveness, in this section, the performance of the proposed LF-SSO is weighted against existing optimization protocol, such as SSO, Cuckoo Search Optimization (CSO), FSO and Genetic Algorithm (GA) centred on end to end delay, packet delivery ratio, EC, throughput, and also network lifetime.

4.1.1. Performance Metrics

End to End Delay (ETED): ETED signifies the time duration that is used-up aimed at transferring a DP as of SNs onto DNs over the network. The ETED is enumerated as as in equation (23),

$$ETED = T'_{(sP)} - T'_{(rP)} \qquad (23)$$

Herein, $T'_{(sP)}$ implies the packet generation time in SN; $T'_{(rP)}$ implies the packet received time in the DN.

Packet Delivery Ratio (PDR): It defines the ratio betwixt the number of DPs supplied to the DN ($N_{r(DP)}$) and the DPs transmitted by the SN ($N_{s(SP)}$)as in equation (24).

$$P_{DR} = \frac{N_{r(DP)}}{N_{s(SP)}} \times 100 \qquad (24)$$

Energy Consumption (EC): It signifies the amount of energy utilized by the network nodes aimed at transferring a DP from SN to DN as in equation (25).

$$E_C = \sum_{n=1}^{d} (E(i)_{initial} - E(i)_{current}) \qquad (25)$$

Here, $E(i)_{initial}$ implies every node's initial energy; $E(i)_{current}$ symbolizes every node's current energy at the simulation's end.

Throughput (Tg): It signifies the average successful delivery of DPs on a destination in specified simulation time as in equation (26).

$$T_g = \frac{\sum N_{r(DP)}}{simulation\ \ time} \times \frac{8}{100} \qquad (26)$$

Network Lifetime (TNL): Time essential aimed at exhausting n-number of mobile nodes' batteries is termed as TNL as in equation (27).

$$T_{NL} = \sum_{n=1}^{d} (E(i)_{current} = 0) \qquad (27)$$

Here, the proposed and existent optimal routing path selection techniques' ETED, PDR, EC, Tg, also and TNL are enumerated by changing the number of nodes as of 20 to 100. Figure 4 exhibits the proposed and existent methodologies' comparison examination.

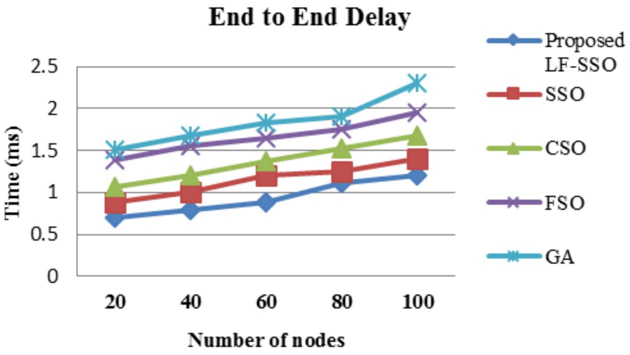


Figure 4 End to End Delay Analysis

Figure-4 analogizes the proposed LF-SSO's performance with the existent protocols, like SSO, CSO, FSO, and GA, regarding ETED. The protocols' ETED are measured in milliseconds. As of figure 4, aimed at 20 nodes, the LF-SSO protocol proposed takes 0.7ms for transferring the DP as of SN to DN, whereas the existent protocols, like SSO, CSO, FSO, and also GA takes 0.89ms, 1.07ms, 1.39ms and 1.51ms aimed at DT. Similarly, for 40, 60, 80, and 100 nodes, the proposed protocol's ETED is much less whilst analogized to the prevalent methodologies. If a transmission delay is incremented, every node's energy gets decremented. As the DP is transferred over the shortest path, the proposed protocol's ETED is low. So, the protocol proposed is greatly effective analogized to the other protocols.

The proposed and existent protocols' PDR aimed at a diverse number of nodes is examined in figure-5. The PDR exhibits how the optimal path selected transfers the DP efficiently as of SN to DN. For effective DT, the protocol's PDR must be high. As of figure 5, it is examined that for 20, 40, 60, 80, and 100 nodes, the proposed protocol attains 0.75, 0.67, 0.89, 0.75, and 0.62 PDR, correspondingly. Nevertheless, the prevalent protocols SSO, CSO, FSO, and GA attains a very less PDR.

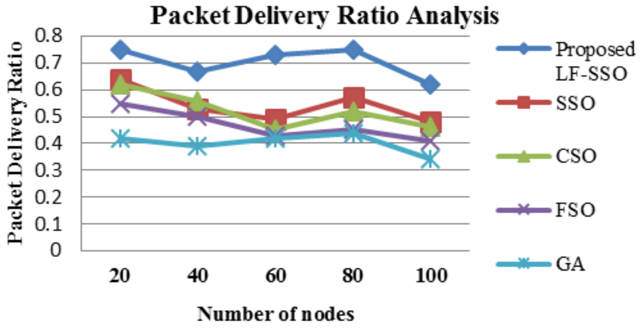


Figure 5 Packet Delivery Ratio Analysis

However, SSO and CSO protocol yield a excellent performance analogized to FSO and GA. The P_{DR}'s low value signifies that the network's QoS isn't effective.

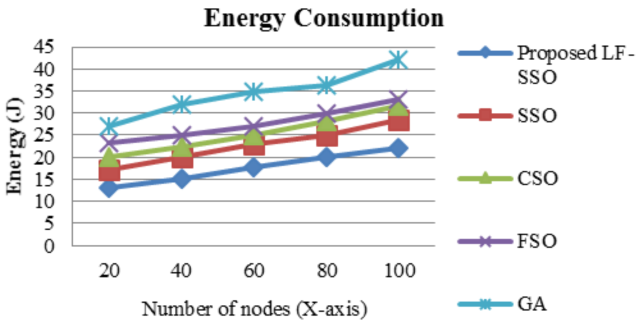


Figure 6 Energy Consumption Analysis

Figure 6 exhibits the EC performance analogy aimed at LF-SSO proposed and existent SSO, CSO, FSO, and GA protocols. The nodes' EC is measured in Joule. Whilst a node consumes greater energy, the DT gets delayed, so the nodes' EC must be less for effective DT. The graph analogy revealed that the proposed LF-SSO's EC is '2' times efficient analogized to the existent GA. For 100 nodes, LF-SSO's EC is 22J, whereas the EC of GA is 42.1J. Other protocols SSO, CSO, FSO spends 28.67J, 31.77J, 33.09J energy at the transmission's end. This analysis clarified that the protocol proposed comprises excellent performance analogized to other procedures.

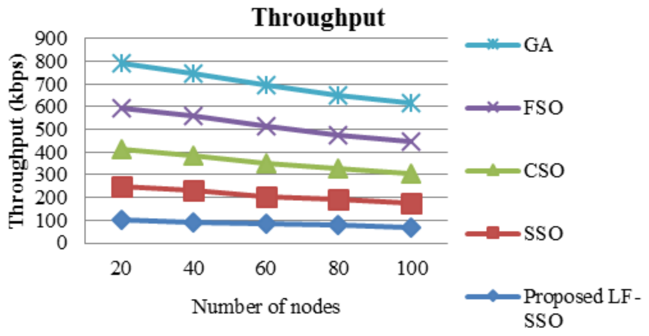


Figure 7 Throughput Analysis

Figure-7 examined the proposed and existent protocols' T_g. Whilst the number of nodes increments, the T_g decrements. As of 20 to 100 nodes, the LF-SSO proposed decrements T_g as of 102kbps to 71kpbs, SSO decrements T_g as of 148kbps to 104kpbs, CSO decrements T_g as of 162kbps to 129kpbs, FSO decrements T_g as of 180kbps to 143kpbs, and GA decrements T_g as of 198kbps to 169kpbs. However, the proposed protocol's T_g is far efficient analogized to other techniques. The minimal route distance offers the benefit of attains a maximal T_g.

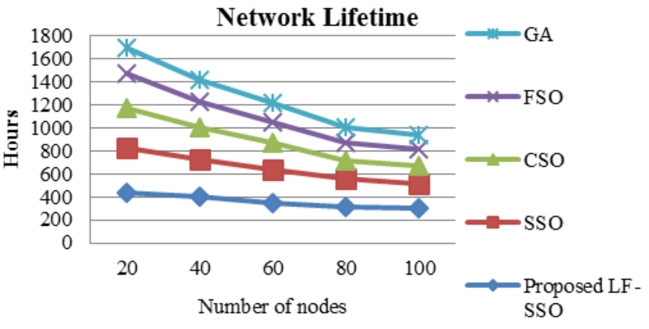


Figure 8 Network Lifetime Analysis

The T_{NL} utilizing the proposed and existent protocols is analogized in figure-8. The number of nodes differs in the (20 to 100) range. The T_{NL} is measured in hours. Performing a DT with 20 nodes, the lifetime of the proposed LF-SSO is 437hrs and the existing SSO, CSO, FSO, and GA protocols are 392hrs, 345hrs, 296hrs, and 230hrs. The T_{NL} utilizing LF-SSO is greater analogized to the existent protocols. Likewise, aimed at the residual count of nodes, the T_{NL} is greater whilst utilizing LF-SSO. Whilst the nodes' EC decremented, the T_{NL} gets incremented. Consequently, this analysis validated that the protocol proposed is extremely effective and excellent analogized to the prevalent protocols.

4.2. Performance Analysis of SH^{2}E

Aimed at preventing DPs as of the DT attacks, the work proposed utilizes the SH^{2}E technique. Here, the proposed cryptography technique's performance is analogized with the existent cryptography techniques, like HE, Elliptic Curve Cryptography (ECC), RSA, and also Diffie-Hellman aimed at validating the proposed technique's security. The performance analogy is examined cntred on encryption time, decryption time, and security level. The encryption time and decryption time is computed by changing the DP size as of 10 kilobytes to 50 kilobytes.

4.2.1. Performance Metrics

Encryption Time (T_e): It signifies the time that is spend aimed at converting the original message (DPs) into ciphertext as in equation (28).

$$T_e = e(T)_{end} - e(T)_{start} \tag{28}$$

Herein, $e(T)_{end}$ signifies the encryption ending time; $e(T)_{start}$ implies the encryption starting time.

Decryption Time (T_d): It signifies the time that is spend aimed at recovering the original message as of the ciphertext as in equation (29).

$$T_d = d(T)_{end} - d(T)_{start} \tag{29}$$

Herein, $d(T)_{end}$ signifies the decryption ending time; $d(T)_{start}$ implies the decryption starting time.

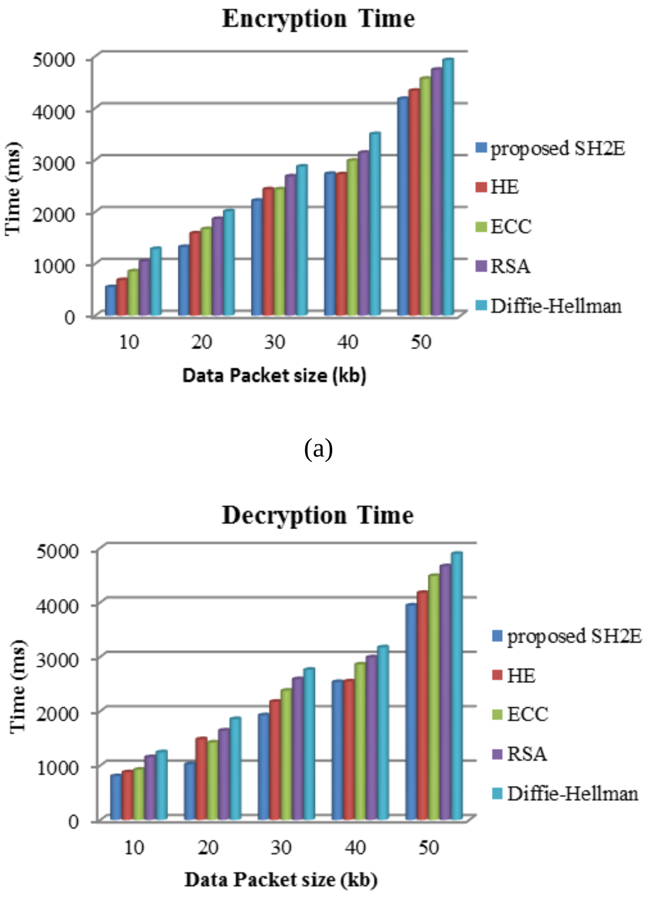
Figure-9 exhibits the comparative analysis of the proposed and existing protocols' performance regarding (a) Te and (b) Td. The performance is gauged grounded on the DP's size (in bytes) ranging as of 10 to 50 kilobytes. Figure-9 validated that the Te and Td increments with the incrementing DP size. Aimed at encrypting a 10kb DP, the SH2E proposed spends 548ms.

However, the existent HE, ECC, RSA, and Diffie-Hellman spends 685ms, 854ms, 1047ms, and 1284ms aimed at encrypting a 64b DP that is greater analogized to the SH2E proposed. Likewise, the SH2E proposed spends lesser time analogized to HE, ECC, RSA, and Diffie-Hellman aimed at the remaining DP size. Like the encryption procedure, in decryption as well, the SH2E proposed spends lesser time analogized to the prevalent algorithms.

Data Packet Size (kilobytes)	Proposed SH2E		HE		ECC		RSA		Diffie-Hellman	
	TE	TD	TE	TD	TE	TD	TE	TD	TE	TD
10	548	803	685	875	854	923	1047	1153	1284	1243
20	1323	1022	1585	1482	1668	1423	1863	1643	2010	1853
30	2214	1923	2434	2172	2434	2376	2684	2587	2873	2760
40	2732	2534	2724	2546	2986	2858	3139	2987	3498	3172
50	4176	3941	4334	4173	4566	4483	4740	4662	4923	4891

Table 3 Performance of Proposed and Existing Cryptographic Algorithms

Aimed at decrypting 10kb to 50kb DPs, the SH^{2}E spends 803ms, 875ms, 923ms, 1153ms, and 1243ms, correspondingly, that is relatively lesser analogized to the prevalent protocols. This analogy validates that the algorithm proposed functions quicker analogized to the existent cryptography technique. The proposed and existent techniques' security level is analogized in figure-10. If any cryptographic technique is utilized aimed at attack prevention, the algorithm must attain a high-security level. On examining the figure, it is clarified that the SH^{2}E algorithm proposed offers 98.54% security level, however the existent HE, ECC, RSA, and Diffie-Hellman offer 95.02%, 92.78%, 89.10%, and 87.28% security level as shown in table 3.



(a)

(b)

Figure 9 Performance Analysis of Proposed and Existing Algorithms Regarding (a) Encryption Time and (b) Decryption Time

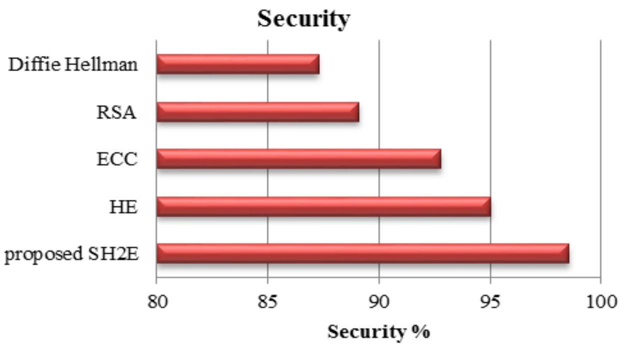


Figure 10 Security Analysis

So, it is validated that the algorithm proposed is extremely efficient and secured analogized to the existent technique. It prevents the DPs as of the DT attacks whilst effectively transmitting the DP as of SN to DN.

5. CONCLUSION

MANET is harshly limited by attacks, storage capacity, computing power, and energy. Consequently, it is vital to build an energy-effective and secured multipath protocol aimed at boosting the TNL and protect the network as of diverse attacks. So, in this work, an LF-SSO and SH2E centred energy-effective secured MR technique is proffered in MANET. The scheme proposed utilizes an LF-SSO aimed at discovering an optimal routing path aimed at an energy-effective secured routing. An SH2E is adapted to boost the DPs' security level against DT attacks. The proposed LF-SSO's ETED, PDR, EC, Tg, and TNL is measured by changing the number of nodes. The proposed SH2E algorithm's Te and Td are also computed for diverse DPs' sizes. As of the performance examination, it is clarified that the techniques proposed are extremely effective and secured analogized to the other existent techniques. The LF-SSO yields PDR up to 0.89 and boosts the TNL up to 437 hours. Conversely, the SH2E technique proposed yields 98.54% security level, and as well it spends just 4176 milliseconds aimed at encrypting the 50kb DP. Hence, the routing scheme proposed was found to be much energy-effective and secured to resist diverse attacks. The TNL and EC are more boosted in the future by utilizing extra node features, like node's bandwidth, as another fitness value.

REFERENCES

[1] Poongothai T and Duraiswamy K, "Intrusion detection in mobile AdHoc networks using machine learning approach", In International Conference on Information Communication and Embedded Systems (ICICES2014), IEEE, pp. 1-5, 2014.

[2] Santosh Kumar Das, and Sachin Tripathi, "Intelligent energy-aware efficient routing for MANET", Wireless Networks, vol. 24, no. 4, pp. 1139-1159, 2018.

[3] De-gan Zhang, Jin-xin Gao, Xiao-huan Liu, Ting Zhang, and De-xin Zhao, "Novel approach of distributed & adaptive trust metrics for MANET", Wireless Networks, vol. 25, no. 6, pp. 3587-3603, 2019.

[4] Rajesh, M., and J. M. Gnanasekar, "Consistently neighbor detection for MANET", In International Conference on Communication and Electronics Systems (ICCES), IEEE, pp. 1-9, 2016, 10.1109/CESYS.2016.7889967.

[5] Muthukumaran, N, "Analyzing throughput of MANET with reduced packet loss", Wireless Personal Communications, vol. 97, no. 1, pp. 565-578, 2017.

[6] De-gan Zhang, Jin-xin Gao, Xiao-huan Liu, Ting Zhang, and De-xin Zhao, "Novel approach of distributed & adaptive trust metrics for MANET", Wireless Networks, vol. 25, no. 6, pp. 3587-3603, 2019.

[7] Anand, M., and T. Sasikala, "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol", Cluster Computing, vol. 22, no. 5, pp. 12681-12687, 2019.

[8] Mohamed Elhoseny, and K. Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique", IEEE Transactions on Reliability, 2019, 10.1109/TR.2019.2915800.

[9] Lakshman Narayana, V, and C. R. Bharathi, "Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs", In Smart Intelligent Computing and Applications, Springer, Singapore, pp. 649-658, 2019, 10.1007/978-981-13-1921-1_63 ·.

[10] Omuwa Oyakhire, and Koichi Gyoda, "Improved proactive routing protocol considering node density using game theory in dense networks", Future Internet, vol. 12, no. 3, pp. 47, 2020.

[11] Burhan Ul Islam Khan, Farhat Anwar, Rashidah Funke Olanrewaju, Bisma Rasool Pampori, and Roohie Naaz Mir, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile adhoc networks", IEEE Access, vol. 8, pp. 124097-124109, 2020, 10.1109/ACCESS.2020.3006043.

[12] Santosh Kumar Das, and Sachin Tripathi, "A nonlinear strategy management approach in software-defined ad hoc network", In Design Frameworks for Wireless Networks, Springer, Singapore, pp. 321-346, 2020, 10.1007/978-981-13-9574-1_14.

[13] Gomathi Krishnasamy, "An energy aware fuzzy trust based clustering with group key management in MANET multicasting", In 2nd International Conference on new Trends in Computing Sciences (ICTCS), IEEE, pp. 1-5, 2019, 10.1109/ICTCS.2019.8923088.

[14] Pushpender Sarao, "Ad Hoc on-demand multipath distance vector based routing in Ad-Hoc Networks", Wireless Personal Communications, pp. 1-21, 2019, 10.4236/cn.2013.53B2075.

[15] Néstor J. Hetnández Marcano, Jonas Gabs Fugl Nørby, and Rune Hylsberg Jacobsen, "On Ad hoc On-Demand distance vector routing in low earth orbit nanosatellite constellations", In IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, pp. 1-6, 2020, 10.1109/VTC2020-Spring48590.2020.9128736.

[16] Sankara Narayanan S., and G. Murugaboopathi, "Modified secure AODV protocol to prevent wormhole attack in MANET", Concurrency and Computation: Practice and Experience, vol. 32, no. 4, pp. e5017, 2020.

[17] Valmik Tilwari, Mhd Nour Hindia, Kaharudin Dimyati, Faizan Qamar, A. Talip, and M. Sofian, "Contention window and residual battery aware multipath routing schemes in mobile ad-hoc networks", International Journal of Technology, vol. 10, no. 7, pp. 1376-1384, 2019.

[18] Tino Merlin R and R. Ravi, "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET", Wireless Personal Communications, vol. 104, no. 4, pp. 1599-1636, 2019.

[19] Sulaiman Abdo Mahyoub Ghaleb, and V. Vasanthi, "Energy efficient multipath routing using multi-objective grey wolf optimizer based dynamic source routing algorithm for MANET", International Journal of Advanced Science and Technology, vol. 29, no. 3, pp. 6096-6117, 2020.

[20] Mariappan Rajashanthi, and K. Valarmathi, "A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs", Wireless Personal Communications, pp. 1-16, 2019, 10.1007/s11277-019-07016-3.

[21] Pattabiram Thulasingam Kasthuribai, and Murugaiyan Sundararajan, "Secured and QoS based energy-aware multipath routing in MANET", Wireless Personal Communications, vol. 101, no. 4, pp. 2349-2364, 2018.

[22] Neenavath Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET", Evolutionary Intelligence, pp. 1-15, 2020, https://doi.org/10.1007/s12065-020-00388-7.

[23] Sannasy Muthurajkumar, Sannasi Ganapathy, Muthuswamy Vijayalakshmi, and Arputharaj Kannan, "An intelligent secured and energy efficient routing algorithm for MANETs", Wireless Personal Communications, vol. 96, no. 2, pp. 1753-1769, 2017.

[24] Aqeel Taha, Raed Alsaqour, Mueen Uddin, Maha Abdelhaq, and Tanzila Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function", IEEE access, vol. 5, pp. 10369-10381, 2017, 10.1109/ACCESS.2017.2707537.

[25] Rajashanthi, M., and Valarmathi K, "Energy-efficient multipath routing in networking aid of clustering with OGFSO algorithm", Soft Computing, pp. 1-10, 2020, 10.1007/s00500-020-04710-4.

[26] Sajal Sarkar, and Raja Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", Ad Hoc Networks, vol. 37, pp. 209-227, 2016.

Authors

Valanto Alappat, obtained his Bachelor's degree in Computer Science from Tamilnadu College of Engineering, Coimbatore, Tamilnadu, India. Then he obtained his Master's degree in Computer & Information Technology from Manonmaniam University, Tirunelveli, Tamilnadu, India and is currently pursuing Ph.D in Computer Science & Engineering from Sathyabama Institute of Science and Technology, Chennai, Tamilnadu, India. Currently, he is an Assistant Professor in Department of Computer Science and Engineering, Thejus Engineering College, Thrissur, Kerala, India. His specializations include Cloud Computing, Bluetooth network, networking, and Ad-hoc networks. His current research interests are Wireless Mesh Networks, Wireless Sensor Networks, Public Key Infrastructure, Network Security, Authentication Server, Virtual Simulation, and heterogeneous wireless networks.

Dr. P. M. Joe Prathap B.E, M.E, Ph.D, obtained his Bachelor's degree in Computer Science & Engineering from St. Xavier's Catholic College of Engineering, Chunkankadai, Tamilnadu, India in 2003, masters from Karunya Institute of Technology, Coimbatore, Tamilnadu, India in 2005 and Ph.D.degree from Anna University, Chennai, India in the year 2011. He has been in the teaching profession for the past 13 years and has handled both UG and PG programmes. He is currently a Professor in the Department of Information Technology, RMD Engineering College, Chennai, Tamilnadu, India. He is a recognized research supervisor of Anna University, St. Peters's University, Sathyabama Institute of Science and Technology & Karpagam University. His research interests are in Computer Networks, Network Security, Operating Systems, Mobile Communication and Data Mining. He is a life member of ISTE & IAENG.

How to cite this article:

Valanto Alappatt, Joe Prathap P M, "Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E", International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 400-411, 2021, DOI: 10.22247/ijcna/2021/209706.